Data Points

Issue 78 December 18, 2007

RDMC Office Move – January 4, 2008

The Research and Data Management Center will be moving its offices on Friday, January 4, 2008. Our new mailing address will be:

Research and Data Management Center
University of Kentucky
1080 Export Street – Suite 200
Lexington, KY 40504.

Phone numbers, FAX numbers, web addresses, etc. will not be changing. Only our mailing address will be different. If you're trying to find our physical office and you need assistance with directions, please contact us.

During the course of the move, our phones, FAXes, data lines, email, and web site will be down. **That includes BPRS/PDA submissions**. We'll be hard to reach. We will be taking everything down on Friday, January 4, at 6:00 AM. We expect to be back up and fully connected to the world by Monday, January 7, at 6:00 AM.

RDMC Holiday Schedule

The Research and Data Management Center offices will be open from December 24 to December 31 (with the exception of Christmas Day and New Years Day) although staffing will be limited. We *will* be processing CMHC data files and providing technical support via email during that time. Technical assistance will be available from amonaghan@rdmc.org or hdhughes@rdmc.org.

Standard timeliness guidelines will apply for the November data files. Submissions need to be finalized by midnight on December 31. Files must be submitted prior to Monday, December 31, at 4:30 PM Eastern Standard Time in order to view the feedback reports prior to month end.

New Web Login Access Form

A Login Access Form for permissions to MHMR.Ky.Gov restricted web pages has been placed in each of the regions' upload directory on the MHMR web site. CMHC staff with data upload permissions should see a document named "LoginAccessForm.doc" under their File Management options. That document can be printed, completed, and sent directly to Frankfort. Instructions are included on the form.

HIPAA and PHI Over Email

As we all know, we need to be careful when sending Protected Health Information via email, especially when sending it outside of one's own network. When dealing with RDMC staff on technical support issues, we need to avoid using SSNs in the body of the email or in unencrypted attachments.

For your reading pleasure, we have included on the following page a posting from the 12/17/2007 issue of the *Weekly HIPAA Advisor* regarding HIPAA requirements for the electronic transfer of PHI.

Enjoy and have a great Christmas!

Q: What level of security does HIPAA require when transmitting patient information electronically (i.e., via the Web, through e-mail, etc.)?

A: It depends on the method used to send the patient information. An organization that transmits the information within its network can send it "clear text" (unencrypted). The organization may choose the level of security it wishes to apply. The same is true for data an organization that transmits via fax-person-to-person versus computer-to-computer-or sends over direct connections.

The answer changes if the organization is sending PHI over an open network (the Internet). Encryption is necessary when organizations send PHI over the Internet or a wireless network.

Different methods of data encryption exist for various communication methods (e.g., secure Web, virtual private network, secure e-mail, etc.). But the bottom line is that HIPAA requires encryption, and the level of encryption should be at least 128 bit encryption (this represents the strength of the encryption algorithm used). Higher levels of encryption are recommended and readily available. The organization's rules for remote access and transmission of PHI over the Internet are as important as its encryption of PHI. It is highly advisable to train all remote users to exercise caution and to be aware of their actions and their surroundings. For example, remote users should avoid working with PHI-even when transmitting data securely via a wireless network-if they are in a public setting where a passerby could see PHI displayed on a computer screen.